Before the

FEDERAL COMMUNICATIONS COMMISSION
445 12th Street SW, Room TW-A325
WASHINGTON, DC 20554
fcc@bcpiweb.com

NOTICE OF PROPSED RULESMAKING
FCC-CIRC1703-02
GN Docket No. 13-111

Prelude Communications

Commission's Secretary, Office of the Secretary,
Federal Communications Commission
First-class, Express, and Priority mail):
445 12th Street, SW
Washington DC 20554

April 28, 2017

In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities

COMMENTS OF PRELUDE COMMUNICATIONS

Prelude Communications (PRELUDE) hereby respectfully submits its consolidated comments on the March 2, 2017 Notice of Proposed Rulemaking of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities by the Federal Communications Commission (Commission) with Publication date on March 31, 2017 in the Federal Register. PRELUDE will comment on the identified Matters outlined in the FCC 34373A1 document. In some cases PRELUDE will provide a brief statement and in others a more detailed response.

BACKGROUND:

PRELUDE has been in the telecommunication business for twenty plus years with a focus on the Correctional Industry. PRELUDE'S CEO is a global expert in the design, development and deployment of over 70 Contraband Interdiction Systems (CIS) type solutions globally and provider of communication interdiction solutions to NATO forces, homeland security agencies that require actionable intelligence. PRELUDE is deeply involved in finding solutions to combat contraband wireless devices while working closely with the correctional agencies, CIS provider of services, commercial carriers and the Federal Communications Commission to ensure all stakeholders' interests are addressed and managed. Related to CIS in the United States of America, PRELUDE's management has provided written testimony to US congress, participated in multiple deployments and installations; one (1) Alpha Pilot, four (4) Beta Pilots, installed two (2) permanent managed access solutions for one of the largest correctional agencies in the United States, secured multiple spectrum agreements with all major carriers and over thirty-five FCC Lease authorizations. In addition, PRELUDE continues to be a thought leader in this area and is dedicated and currently working closely with industry leaders to eliminate the use of contraband wireless devices for criminal activity, which is a serious threat to the safety of prison employees, other prisoners, and the general public.

Since inmates circumvent the currently installed communications systems, including authorized calling lists, monitoring, recording and tracking of data for but not limited to controlling criminal activity through contraband wireless devices, PRELUDE believes the objective is to stop the unauthorized and uncontrollable communications by inmates. Although PRELUDE believes managed access systems can be an effective at controlling the use of contraband wireless devices, PRELUDE also believes it is important to have various technologies available to the correctional agencies to provide a layered security solution to combat the use of contraband wireless devices. These various technologies range in effectiveness and efficiencies (including labor and price). Only the correctional agency can determine the value and benefit of each of the independent technologies or as a combined solution. In addition, PRELUDE understands that the agencies as well as the commercial carriers will have to invest time and money to increase Services will not stop the inmates from communicating using contraband wireless devices; they will only hinder use for a limited time until new contraband wireless devices or SIM cards can be used. Also, blocking at the network level does not prevent communications over Wi-Fi or other non-cellular communication protocols which could be active at the facility, once the network denial of service is implemented and successful.

PRELUDE is aware that MAS and contraband assessments services at several facilities across the country and has found evidence to suggest that terminating service at the macro-level would have little to no impact on the inmates inside the facilities. When we analyze the data produced from many of these assessments, we find that many locations have devices where the IMEI field produces all zeros (000000000000000) as well as the presence of phones that change their IMEI each time the phone is turned on, which would only allow the carrier to block the SIM card for these devices. The data also suggests that devices, which are SIM-based are preferred in locations where access to these types of carriers exist (most). And most offenders who have SIM's, have multiple SIMs, and can quickly replace the SIM with another until the new SIM is identified and blocked in the network. Further analysis shows that inmates are swapping SIM cards quite frequently inside the institutions including devices that are wiped, and moved from housing unit to housing units.

IV. FURTHER NOTICE OF PROPOSED RULEMAKING

I. Disabling Contraband Wireless Devices in Correctional Facilities

86. *Discussion.*

We recognize that wireless providers favor a court-ordered termination process as an alternative, but we believe that requiring court orders would be unnecessarily burdensome and that Commission rule-directed disabling should be sufficient to address concerns about liability. *PRELUDES COMMENTS: We as a technology provider of CIS and Provider of Service to correctional agencies support the CMRS concerns about liability and privacy related concerns. The FCC should adopt rules ensuring CMRS, CIS and Provider of Service are protected from liability and legal issues related to the identification, capture and denial of service of wireless communication devices captured in the course of normal operations at a correctional/law enforcement facility.*

Until recently, we believed that a MAS/CIS solution can and would be the best for all stakeholders. With the disappointing results and developments with MAS solutions deployed over the last 48 months and the lack of financial resources available by the correctional agencies, it has become clear, that a network based solution is required to provide an affordable alternative to MAS. Also, due to inexperienced individuals and firms who either do not know the correctional market space, and or have little to no experience with CIS type solution, the correctional industry is searching for an effective and affordable solution which could be installed and operational in weeks.

We note that the current record does not sufficiently demonstrate that reliance on the wireless providers' alternative court-ordered approach in lieu of the proposed rule-based approach discussed below would achieve one of the Commission's overall goals in this proceeding of facilitating a comprehensive, nationwide solution. *PRELUDES COMMENTS: We are currently working closely with a department of corrections and CMRS to develop a process to ensure an effective solution for all stakeholders.*

We also note that the record does not reflect persuasive evidence of successful voluntary termination of service to contraband wireless devices in correctional facilities by the CMRS licensees, even where there is evidence of a growing problem. *PRELUDES COMMENTS: We are currently working closely with a department of corrections and CMRS to develop a process to ensure an effective solution for all stakeholders and believe a court order to denial service to contraband devices will be forthcoming and acceptable to CMRS and State and Local agencies.*

87. To the extent commenters continue to support a court-ordered approach, we seek specific comment on the particulars of the requested court-ordered process to evaluate and compare it to our proposal: who is qualified to seek a court order and with what specific information or evidence? *PRELUDES COMMENTS: We have a working group and in progress of working the details. An updated will be provided at a later date.*

Additionally, given the trey acknowledged nationwide scope and growth of the contraband wireless device problem, how would CIS and wireless providers navigate the myriad fora through which requests for termination might flow, potentially requiring engagement with a wide variety of state or federal district attorneys' offices; federal, state or county courts; or local magistrates? *PRELUDES COMMENTS: We in progress of working the details. An updated will be provided at a later date.*

In this regard, we seek examples of successfully issued and implemented court orders terminating service to contraband wireless devices, as well as demonstrations that court orders can be effective at scale and not overly burdensome or time-consuming to obtain and effectuate in this context. *PRELUDES COMMENTS: We have an active working group and in progress of working the details. An updated will be provided at a later date.*

88. *Commission Authority.*
We believe that Section 303 provides the Commission authority to adopt rules requiring CMRS carriers to disable contraband wireless devices as discussed in detail below. Pursuant to Section 303(b), the Commission is required to "[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class." Additionally, Section 303(d) requires the Commission to "[d]etermine the location of classes of stations or individual stations, "and Section 303(h) grants the Commission the "authority to establish areas or zones to be served by any station." When tied together with Section 303(r), which requires the Commission to "[m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter," we believe that these provisions empower the Commission to implement this proposal. *PRELUDES COMMENTS: We support the Commissions streamline authority to enable contraband device denial of service in network. We as a technology provider of CIS and Provider of Service to correctional agencies support the CMRS concerns about liability and privacy related concerns. The FCC should adopt rules ensuring CMRS, CIS and Provider of Service are protected from liability and legal issues related to the identification, capture and denial of service of wireless communication devices captured in the course of normal operations at a correctional/law enforcement facility on a Federal, State and Local level.*

91. *Disabling of Contraband Wireless Devices in Correctional Facilities.* We propose rules in this Further Notice mandating that CMRS licensees disable contraband wireless devices in correctional facilities detected by an eligible CIS when they receive a qualifying request from an authorized party.

We clarify that CIS systems operating solely to prevent calls and other communications from contraband wireless devices, described in the *Notice* as MASs, will not be subject to these eligibility criteria, unless the department of corrections/CIS provider seeks to use the information received from such a system to request, through Commission rules, contraband wireless device disabling. *PRELUDES COMMENTS: We know that MAS solutions cost grow unsustainably high as effectiveness rises in to high (>95%). The challenge is driven by the fact that 95% facility coverage is far from 95% effectiveness. The inmates have unlimited time to find those area where the system is not effective and use the phones in those areas. It is Prelude experience that inmates will use improvised shielding to try and create reception directivity to circumvent MAS coverage. Which mean that effective MAS deployment over provision to address both inmate activity as well as shifting Macro network power and frequency changes.*

Prelude suggests that all MAS solutions are required to meet minimum eligibility criteria. Furthermore, cost effective MAS deployment should use DoS in network as a means to prevent selected contraband devices from circumventing the MAS solution.

99. After careful consideration of the record, we propose in this Further Notice rules mandating that CMRS licensees disable contraband wireless devices in correctional facilities detected by an eligible CIS pursuant to a qualifying request that includes, *inter alia*, specific identifying information regarding the device and the correctional facility. As discussed below, in proposing that a qualifying request must include unique device identifiers, we seek to ensure that the disabling process will completely disable the contraband device itself and render it unusable, not simply terminate service to the device as we had originally proposed in the *Notice*. Our proposed process includes a required FCC determination of eligibility of CISs to ensure the systems satisfy minimum performance standards, appropriate means of requesting the disabling, and specifics regarding the required carrier response. We seek specific comment on all aspects of the process as well as the costs and benefits of their implementation. *PRELUDES COMMENTS: We support this process and can provide accurate data to ensure the contraband devices are identified at the facilities to either DoS and or completely disabling contraband devices in near real time. The cost to capture the unique identifier can be as low as a few thousands of dollars per month and higher depending on the objectives of the agency. We believe that disabling contraband devices from the network will be (1) limited in scope as devices are easily sourced from abroad (2) introducing such a feature creates an inherent vulnerability for all cellphone users (3) calls for an unrealistic cooperation between cellphone manufacturers and operators on a global scale.*

100. *Eligibility of CISs.* In proposing to mandate the disabling of contraband wireless devices in correctional facilities, we seek to ensure that the systems detecting contraband wireless devices first meet certain minimum performance standards in order to minimize the risk of disabling a non-contraband wireless device. We propose to determine in advance whether a CIS meets the threshold for eligibility to be the basis for a subsequent qualifying request for device disabling, which will facilitate contracts between stakeholders, for example departments of corrections and CIS providers, and appropriate spectrum leasing arrangements, typically between CIS providers and wireless providers. We envision that this eligibility determination would not at this stage assess the CIS's characteristics related to a specific deployment at a certain correctional facility, but rather a CIS's overall methodology for system design and data analysis that could be included in a qualifying request, where more specific requirements must be met for device disabling. We therefore propose that CIS operators seeking wireless provider disabling of contraband wireless devices in a correctional facility must first be deemed an eligible CIS by the Commission, and we intend to periodically issue public notices listing all eligible CISs. In order to be deemed eligible, a CIS operator must demonstrate the following: (1) all radio transmitters used as part of the CIS have appropriate equipment authorization pursuant to Commission rules; (2) the CIS is designed and will be configured to locate devices solely within a correctional facility, can secure and protect the collected information, and is capable of being programmed not to interfere with emergency 911 calls; and (3) the methodology to be used in analyzing data collected by the CIS is sufficiently robust to provide a high degree of certainty that the particular wireless device subject to a later disabling request is in fact located within a correctional facility. We seek comment on the appropriate format for requesting eligibility, taking into consideration our goal of reducing burdens and increasing administrative efficiency. *PRELUDES COMMENTS: We support process of eligibility of CISs, but would suggest it MUST include all CIS and MAS related products and services. The current CIS vendors and or provider of service to the correctional over the last 48 months overall have been fair to poor at best (with exception of two solution provider) and deployed solutions which were not either designed to expand to new protocols, ineffective RF antenna systems which had multiple holes in coverage, and a lack of knowledge related to cellular interdiction capabilities and technology. These as well as other problems have created negative feelings towards MAS over the last 48 months and the need for other alternative solutions.*

101. Given the extensive CIS eligibility criteria, representing the initial requirement for making a qualifying request described in this proposal, we believe it is unlikely that any significant number of non-contraband devices will be erroneously detected and actually disabled. However, we seek further comment on the costs, benefits, and burdens to potential stakeholders of requiring CIS eligibility before qualifying disabling requests can be made to wireless providers. We believe that our proposed eligibility criteria adequately address concerns expressed in the record regarding improper functioning of CIS systems and inaccurately identifying contraband devices. If commenters disagree, we seek comment on what additional eligibility criteria would ensure the accuracy and authenticity of CISs.

For example, should we require testing or demonstrations at a specific correctional facility prior to making a CIS eligibility determination? *PRELUDES COMMENTS: YES*

If testing were part of a general eligibility assessment, would such additional testing at a specific site be unduly burdensome or unnecessarily delay or undermine either state RFP processes or spectrum lease negotiations? *PRELUDES COMMENTS: Additional testing should always be part of a new solution deployment as well as periodic review when dealing with active base stations. The CMRS, correctional agencies, correctional agency service providers (ITS vendors) all needs to ensure that experienced and knowledgeable firms and individuals are selected.*

Should we require that a CIS be able to identify the location of a wireless device to within a certain distance? *PRELUDES COMMENTS: With the correct design of the RF Antenna solution and or Identification Location system, and based on facility property lines and policies, technology is available today to provide a high level of confidence and accuracy to identify contraband devices in use is selected areas, zones, housing units and facilities. The amount of sensors and or related technology has a direct impact on costs with current technology solutions. We suggest this distance issue be tabled until more data is available to make a well informed determination, based on new solutions either in development or being deployed. Furthermore, different facilities have unique needs and budgets, setting such a requirement would limit facilities in procuring the right solution for their needs.*

Is such an accuracy requirement unnecessary or would it be beneficial in assessing the merits of a CIS design and reducing the risk of capturing non-contraband devices? *PRELUDES COMMENTS: YES, accuracy requirements are necessary and beneficial in assessing the merits of a CIS vendor and technology, the distance or plus / minus is to be determined. With the correct design of the RF Antenna solution and or Identification Location system, and based on facility property lines and policies, technology is available today to provide a high level of confidence and accuracy to identify contraband devices in use is selected areas, zones, housing units and facilities. We suggest this distance issue be tabled until more data is available to make a well informed determination.*

Should any eligibility determination be subject to a temporal component, for example, requiring a representation on an annual basis that the basic system design and data analysis methodology have not materially changed, and should the CIS operator be required to provide the Commission with periodic updates on substantial system changes, upgrades or redesign of location technology? *PRELUDES COMMENTS: Depending on the solution deployed, fixed, mobile, and or assessment type solution will determine how best to handle and or if required steps to assure an accurate solution.*

Should eligibility be contingent on the submission of periodic reports detailing any incidents during the applicable period where devices were erroneously disabled? *PRELUDES COMMENTS: We believe that a correctly deployed solution will include audit and or logs/reports detailing contraband as wells an erroneously captured devices, and details related to actions to cure.*

Should the eligibility criteria be different depending on whether the facility is in a rural or urban area, or whether the CIS provider, the correctional facility, or the CMRS licensee is large or small? *PRELUDES COMMENTS: Eligibility criteria should be the same for CIS provider, and solution deployed should be tailor or designed to meet agencies requirements, including if rural, suburban and or urban areas.*

102. *Qualifying Request.* In addition to ensuring that CISs meet certain performance standards in order to minimize the risk of error, we also seek to ensure that an authorized party provides the information necessary for a wireless provider to disable contraband wireless devices. We propose to require that CMRS licensees comply with our proposed disabling process upon receipt of a qualifying request made in writing and transmitted via a verifiable transmission mechanism. We seek comment on whether the qualifying request must be transmitted (1) by the Commission (including, potentially, by the contraband wireless device ombudsperson referenced above), upon the request of a Designated Correctional Facility Official (DCFO), which we propose to define as a state or local official responsible for the facility where the contraband device is located; or (2) by the DCFO. We acknowledge that a request transmitted directly from a DCFO to the CMRS licensee, after a CIS is deemed eligible and expressly pursuant to a Commission rule, may be made more timely and efficiently than a request transmitted from the DCFO to the Commission, and then to the CMRS licensee. We seek specific comment on our proposed definition of DCFO, as well as the costs and benefits of these two approaches to the transmission of the qualifying request, both in terms of timeliness and any perceived liability concerns. *PRELUDES COMMENTS: We believe that to have an effective solution with CMRS Denial of Service and device blocking in network, timing is critical and this process needs to happen as fast as possible, and only near real time is acceptable. Technology is available today to identify, capture and transmit the unique contraband devices data in near real time to CMRS. The goal is to deliver this data to CMRS electorally and disable within minutes or second, preventing unauthorized communications in correctional facilities. The DCFO should be able to designate an agent/representative whose sole focus is managing and handling the information gathered by on-site appliance solution of the CIS vendor.*

104. We propose that in order for the request to disable a contraband wireless device to be a qualifying request, the DCFO must make a number of certifications and include device and correctional facility information. Specifically, we propose that the DCFO must certify in the qualifying request that (1) an eligible CIS was used in the correctional facility, and include evidence of such eligibility; (2) the CIS is authorized for operation through a license or Commission approved lease agreement, referencing the applicable ULS identifying information; (3) the DCFO has contacted all CMRS licensees providing service in the area of the correctional facility for which it will seek device disabling in order to establish a verifiable transmission mechanism for making qualifying requests and for receiving notifications from the licensee; and (4) it has substantial evidence that the contraband wireless device was used in the correctional facility, and that such use was observed within the 30 day period immediately prior to the date of submitting the request. We seek comment on these requirements and any methods in which the Commission can facilitate interaction between the authorized party and the CMRS licensees during the design, deployment, and testing of CISs. For example, would it be useful for the Commission to maintain a list of DCFOs? What role could the contraband ombudsperson play in facilitating the interaction between DCFOs and CMRS licensees? *PRELUDES COMMENTS: We believe the DCFO must have the ability to select an agent or representative to handle the above and or similar responsibilities, and to ensure and effective near real time solution. We must have a streamline process which assume items 1, 2, 3 and 4 are in compliance and the requests from DCFO to CMRS to disable contraband device happens in near real time, and items 1-4 are best practices which need to be confirmed in advance of the 1st request, and on an annual or periodic basis.*

105. Finally, we propose that a qualifying request must include specific identifying information regarding the device and the correctional facility. We propose that the request include device identifiers sufficient to

uniquely describe the device in question and the licensee providing CMRS service to the device. We seek comment on whether the proposal to include the CMRS licensee is only warranted if the request is made directly to the Commission, and potentially unnecessary if the request is made directly from a DCFO to the CMRS licensee able to confirm that the device is a subscriber on its network. *PRELUDES COMMENTS: Unique device information includes the subscriber network and carrier. We see no reason why the Commission should be included in this process.*

With regard to device identifiers, we seek specific comment on whether other details are necessary in addition to identifiers that uniquely describe the specific devices, such as make and model of the device or the mode of device utilization at the time of detection. Is it relevant whether the device – at the time of detection – was making an incoming or outgoing voice call, incoming or outgoing SMS text or MMS (multimedia) message, or downloading or uploading data? *PRELUDES COMMENTS: We believe that the following are required to disable contraband devices in CMRS networks. Facility Location, CIS type of technology (fixed, mobile or assessment), CIS Provider of Service, Contraband Device data (hardware and SIM identifiers and subscriber network) and other (court order reference numbers, etc.). We recognize that equipment number may be spoofed (some custom firmware support this function) leading to different procedure to classify contraband SIM (IMSI) as contraband than those needed to classify equipment as contraband.*

106. We seek additional comment on whether other details are necessary in terms of location and time identifiers, such as latitude and longitude to the nearest tenth of a second, or frequency band(s) of usage during the detection period, in order to accurately identify and disable the device. Is it necessary to require that a request include specific identifiers to accurately identify and disable the device, or would providing the flexibility to include alternative information to accommodate changes in technology be appropriate, and what types of alternative information would further our goal of an efficient disabling process? Specifically, what is necessary to accurately identify and disable the device? For example, common mobile identifiers include international mobile equipment identifier (IMEI) and the international mobile subscriber identity (IMSI), used by GSM, UMTS, and LTE devices; and electronic serial number (ESN), mobile identification number (MIN), and mobile directory number (MDN), used by CDMA devices. Should additional information be required to accurately identify a specific wireless device for requested disabling? Are there significant differences in the identifying information of current wireless devices (e.g., android, iOS, windows) that must be accounted for? We seek to minimize burdens for those providing information, by only requiring what is essential to properly disable. *PRELUDES COMMENTS: The minimum data required to support stakeholder's objective and concerns.*

107. We seek comment on whether there are commonalities that would permit standardized information sharing, while still taking into account the full range of devices, operating systems, and carriers. We also seek comment on the appropriate format of a qualifying request to streamline the process and reduce administrative burdens. Would it be more efficient for carriers to develop a common data format so that corrections facilities, through a DCFO, are not required to develop a different format for each wireless provider? Should any of these requirements vary depending on whether the wireless provider is small or large? *PRELUDES COMMENTS: A standardized of information sharing is required to ensure a near real time denial of service in carrier network....manual / human intervention will hinder an effective solution.*

108. In comments, Tecore raises the concern that SIM cards can be easily replaced so that devices are only temporarily deactivated. After review of the record, we recognize that termination of service alone may be an incomplete solution capable of inmate exploitation. Today, we propose disabling rules as a potentially more effective approach to ensure that not only is service terminated to the detected contraband device, but also that the device is rendered unusable on that carrier's network. We seek comment on the technical feasibility of this proposed disabling requirement, including the costs and

benefits of implementing such a requirement. We also seek comment on the implications of proposed disabling on 911 calls. We note that a disabled device will not have 911 calling capability, whereas a service terminated device would maintain 911 calling capability pursuant to the Commission's current rules regarding non-service initialized (NSI) phones. While today we propose to require contraband wireless device disabling, should we nonetheless maintain the requirement that CMRS carriers keep 911 capability for such disabled contraband phones, subject to the outcome of the NSI proceeding? What are the costs and benefits to stakeholders of such a requirement? *PRELUDES COMMENTS: We support the denial of service and blocking the device from operating on the network and can provide data to support. Assuming agency and PSAP do not want 911 call handling on contraband devices, we see not issue with 911. Authorized devices in area will be able to make 911 calls.*

109. We propose that a qualifying request must also include correctional facility identifiers, including the name of the correctional facility, the street address of the correctional facility, the latitude and longitude coordinates sufficient to describe the boundaries of the correctional facility, and the call signs of the Commission licenses and/or leases authorizing the CIS. We seek comment on whether this information will provide sufficiently accurate information about the correctional facility to ensure that the carrier can restrict the disabling of wireless devices to those that are located within that facility. *PRELUDES COMMENTS: NO, this data should be included with the CMRS spectrum and other related agreements on file and are not necessary on a per device request.*

110. *Disabling Process.* As a preliminary matter, we propose to require that the CMRS licensee must provide a point of contact suitable for receiving qualifying requests to disable contraband wireless devices in correctional facilities. We seek to ensure that such requests can be transmitted in an expeditious manner and to have confidence that the request will be received and acted upon. We seek comment on this proposal. *PRELUDES COMMENTS: We believe that after confirmation of the CIS technology, CIS Provider of Service and Correctional Agency the disabling process must be done electronically and not relay on human intervention which will delay and hinder the process. The capabilities exist and only need to be given access for software integration.*

111. We recognize the need to safeguard legitimate devices from being disabled. Accordingly, we seek comment on what steps, if any, the CMRS licensee should be required to take to verify the information received, whether customer outreach should be part of the process, and the time frame within which the steps must be taken. We seek information to assist us in determining what level of carrier investigation, if any, should be required to determine whether there is clear evidence that the device sought to be disabled is not contraband. We also seek comment on what level of customer outreach, if any, should be required to ensure that the disabling request is not erroneous. *PRELUDES COMMENTS: Once the CIS and CIS Provider of Service has accepted by CMRS, Agency and that testing / pilot data has been reviewed, confirmed by CMRS and modified to meet standards...the CMRS should block / deny service to the contraband device within seconds. Any erroneous device information which was block, the CIS vendor data sent to CRMS must have process and systems in place to address with CMRS and unblock/deny with supporting data.*

113. With regard to customer outreach, we again seek comment on a range of approaches, including requiring immediate disabling without any customer outreach, or requiring the carrier to contact the subscriber of record through any available means (e.g., text, phone, email) and provide a reasonable amount of time prior to disabling for the customer to demonstrate that the disabling request is in error.
We seek comment on whether a particular alternative enables inmates to evade device disabling. Each of these approaches impacts carrier response time and the ability to address, however unlikely, disabling errors. If we require some level of carrier investigation or customer outreach, we provide the CMRS licensees a method to reject a qualifying request if it is determined the wireless device in question is not

contraband. *PRELUDES COMMENTS: We do not believe that customer outreach is required with the correct deployment of technology by CIS vendors. The key objective is to disable communications in the most timely fashions and outreach will delay this process. The testing and technology confirmation should provide enough confidence and accuracy to CMRS.*

114. We also propose that the CMRS licensee must provide notification to the DCFO within a reasonable time period that it has either disabled the device or rejected the request. We seek comment on what the reasonable time period should be for this notification, whether the licensee must provide an explanation for the rejection, and whether the DCFO can contest the rejection. We seek comment on all aspects of the disabling process regarding verification of disabling requests, particularly the costs and benefits to the wireless providers, CIS operators, and the correctional facilities. *PRELUDES COMMENTS: All requests to disable must be completed in an agreed upon time. No devices should be rejected base on public safety.*

117. Finally, we believe that the FCC process for determining CIS eligibility discussed above will substantially ensure that only contraband wireless devices located within correctional facilities are identified for carrier disabling. At the same time, we believe it is worthwhile to seek comment on the methods that would be available to wireless providers to minimize any impact on customers whose devices are not located within a correctional facility. We seek comment on the costs and burdens associated with establishing a process to overcome any such instances. Are there contractual provisions in existing contracts between CMRS providers and their customers that address this or similar issues? We also seek comment on what period of time would be reasonable to expect a CMRS licensee to reactivate a disabled device. For example, what methods of discovery will sufficiently confirm that a wireless device is not contraband? Is 24 hours a reasonable period to resolve potential errors and how extensive is the burden on subscribers to remain disabled for that period? What is the most efficient method of notifying the carriers of errors, if originating from parties outside a correctional facility, and of notifying subscribers of reactivation? *PRELUDES COMMENTS: We believe that the CIS provider of Service and or CMRS should have a process to address contraband devices which were accurately identified as contraband devices within a correctional facility, that have moved from inside to outside the secure area by staff, officers and or visitors. If a contraband device subscriber claims they were mistakenly denied service and the device is no longer in the facility, the CMRS can use network data location services to locate if the device in question is no longer near the facility.*

118. In the *Notice*, the Commission also sought comment on Cell Antenna's proposal that we adopt a rule to insulate carriers from any legal liability for wrongful termination, while noting that wireless carriers' current end user licensing agreements may already protect the carriers. We seek further comment on this proposal. Specifically, we seek comment on whether the Commission should create a safe harbor by rule for wireless providers that comply with the federal process for disabling phones in correctional facilities. How broadly should that safe harbor be written, and should it apply only to wireless providers that comply with every aspect of the rules we adopt or also those that act in good faith to carry out the disablement process? Does the Commission have authority to adopt a safe harbor? Is our authority to adopt the rules at issue sufficient to create a safe harbor? Are there other provisions of the Communications Act not previously discussed that would authorize a safe harbor? And what, if any, downsides are there to creating a safe harbor for wireless providers that comply with federal law? *PRELUDES COMMENTS: We support CIS and CMRS safe harbor from all risk and liability concerns related to contraband devices in correctional facilities and either blocking on site or at the CMRS network.*